Towards *Interactive* Belief, Knowledge & Provability: Possible Application to *Zero-Knowledge Proofs*

➡ Ph.D. Thesis Chapter 5

Simon Kramer

December 18, 2007

Target audience: Cryptographers, Computer Scientists, Logicians, Philosophers

Overall Argument

1. **Zero-Knowledge proofs** have a *natural* (logical) formulation in terms of *modal* logic.
2. ***Modal* operators** of ***interactive belief***, ***knowledge***, and ***provability*** are definable as natural generalisations of their ***non-*interactive** counterparts.

Overview

1. Introduction
   i. Motivation
   ii. Goal
   iii. Prerequisites
      - *individual* knowledge
      - *propositional* Knowledge
      - spatial implication
      - evidence & Belief, proof & Provability
      - epistemic implication
2. *Interactive* individual knowledge, proof & Provability
3. Application to Zero-Knowledge proofs
4. *Interactive* evidence & Belief
5. Conclusion

Introduction

Motivation

How to redefine modern cryptography in terms of modal logic?

probabilistic polynomial-time Turing-machines

➡ *low*-level & *operational* definitions (*how*)

➡ mentally intractable proofs

➡ Modern cryptography is cryptic.

How to generalise non-interactive modal concepts to the interactive setting? [van Benthem]

from monologue to dialogue

➡ rational agency (game theory)

Introduction

Goal

To redefine modern cryptography in terms of modal logic

- ➡ *high*-level & *declarative* definitions (*what*)
- ➡ mentally tractable proofs
- ➡ Logical cryptology.

To define **interactive** belief, knowledge, and provability

- ➡ building blocks for rational agency

Introduction
Prerequisites (1/5)

***Individual* knowledge (knowledge of *messages*):**

- *name generation*
- message *reception*
- message *analysis*
- message *synthesis*

via message analysis

$$\frac{\mathtt{Eve}\ \mathsf{k}\ \{\!|M|\!\}_k \qquad \mathtt{Eve}\ \mathsf{k}\ k}{\mathtt{Eve}\ \mathsf{k}\ M}$$

via message synthesis

$$\frac{\mathtt{Eve}\ \mathsf{k}\ M \qquad \mathtt{Eve}\ \mathsf{k}\ k}{\mathtt{Eve}\ \mathsf{k}\ \{\!|M|\!\}_k}$$

Introduction

Prerequisites (2/5)

Propositional Knowledge (Knowledge of the truth of propositions) — almost:

K	$\models \mathsf{K}_b(\phi \rightarrow \phi') \rightarrow (\mathsf{K}_b(\phi) \rightarrow \mathsf{K}_b(\phi'))$
T	$\models \mathsf{K}_b(\phi) \rightarrow \phi$
4	$\models \mathsf{K}_b(\phi) \rightarrow \mathsf{K}_b(\mathsf{K}_b(\phi))$
5	$\models \neg\mathsf{K}_b(\phi) \rightarrow \mathsf{K}_b(\neg\mathsf{K}_b(\phi))$
N	$\dfrac{\models \phi}{\models \mathsf{K}_b(\phi)}$

Introduction
Prerequisites (3/5)

Spatial implication (assume — guarantee):

$\mathfrak{s} \models \phi \triangleright \phi' \quad$:iff $\quad$ for all extensions $\mathfrak{s}''$ of $\mathfrak{s}$ by $\mathfrak{s}'$, if $\mathfrak{s}' \models \phi$ then $\mathfrak{s}'' \models \phi'$

$$\langle \epsilon \cdot \mathtt{I}(\mathtt{Eve}, \{\!|M|\!\}_k), P\rangle \models \mathtt{Eve}\ \mathsf{k}\ k \triangleright \mathtt{Eve}\ \mathsf{k}\ M$$

$\models \mathtt{Eve}\ \mathsf{k}\ M \triangleright \mathtt{Eve}\ \mathsf{k}\ M \qquad \not\models \neg\mathtt{Eve}\ \mathsf{k}\ M \triangleright \neg\mathtt{Eve}\ \mathsf{k}\ M$

Introduction

Prerequisites (4/5)

Theorem: P_a is S4

Provability (other than Artëmov's) & proof:

$$\mathsf{P}_b(\phi) := \exists m(m \; \mathsf{proofFor} \; \phi \wedge b \; \mathsf{k} \; m)$$

$$m \; \mathsf{proofFor} \; \phi := \forall(c : \mathtt{A}_{\mathtt{Adv}})(c \; \mathsf{k} \; m \rhd \mathsf{K}_c(\phi))$$

Theorem: B_a is KD4

Belief and evidence:

$$m \; \mathsf{evidenceFor} \; \phi := \forall(c : \mathtt{A}_{\mathtt{Adv}})(\mathsf{K}_c(\phi) \rhd c \; \mathsf{k} \; m)$$

$$\mathsf{B}_b(\phi) := \exists m(m \; \mathsf{evidenceFor} \; \phi \wedge b \; \mathsf{k} \; m)$$

Introduction

Prerequisites (5/5)

Epistemic **implication (*if — then possibly because*):**

$$\langle \epsilon \cdot \mathtt{I}(\mathtt{Eve}, \{\!|M|\!\}_k) \cdot \mathtt{I}(\mathtt{Eve}, k), P\rangle \models \mathtt{Eve}\ \mathsf{k}\ M \supseteq \mathtt{Eve}\ \mathsf{k}\ k$$

Derivation of individual knowledge

$$\dfrac{\dfrac{\dfrac{}{\epsilon \cdot \mathtt{I}(\mathtt{Eve}, \{\!|M|\!\}_k) \cdot \mathtt{I}(\mathtt{Eve}, k) \vdash^{\{\mathtt{I}(\mathtt{Eve},k)\}}_{\mathtt{Eve}} (\mathtt{Eve}, k)}}{\epsilon \cdot \mathtt{I}(\mathtt{Eve}, \{\!|M|\!\}_k) \cdot \mathtt{I}(\mathtt{Eve}, k) \vdash^{\{\mathtt{I}(\mathtt{Eve},k)\}}_{\mathtt{Eve}} k} \qquad \dfrac{\dfrac{\dfrac{}{\epsilon \cdot \mathtt{I}(\mathtt{Eve}, \{\!|M|\!\}_k) \vdash^{\{\mathtt{I}(\mathtt{Eve},\{\!|M|\!\}_k)\}}_{\mathtt{Eve}} (\mathtt{Eve}, \{\!|M|\!\}_k)}}{\epsilon \cdot \mathtt{I}(\mathtt{Eve}, \{\!|M|\!\}_k) \vdash^{\{\mathtt{I}(\mathtt{Eve},\{\!|M|\!\}_k)\}}_{\mathtt{Eve}} \{\!|M|\!\}_k}}{\epsilon \cdot \mathtt{I}(\mathtt{Eve}, \{\!|M|\!\}_k) \cdot \mathtt{I}(\mathtt{Eve}, k) \vdash^{\{\mathtt{I}(\mathtt{Eve},\{\!|M|\!\}_k)\}}_{\mathtt{Eve}} \{\!|M|\!\}_k}}{\epsilon \cdot \mathtt{I}(\mathtt{Eve}, \{\!|M|\!\}_k) \cdot \mathtt{I}(\mathtt{Eve}, k) \vdash^{\{\mathtt{I}(\mathtt{Eve},k), \mathtt{I}(\mathtt{Eve},\{\!|M|\!\}_k)\}}_{\mathtt{Eve}} M}$$

Interactive individual knowledge, proof & Provability

Interactive individual knowledge

$$M' \supseteq_{(a,b)} M := b \mathsf{k} M' \wedge (b \mathsf{k} M' \supseteq a \mathsf{k} M)$$

2-party *interactive* proof

$$\begin{array}{rcl} M \ \mathsf{iProofFor}_{(a,b)} \ \phi & := & M \ \mathsf{iProofFor}^{a}_{(a,b)} \ \phi \\ (M, \blacksquare) \ \mathsf{iProofFor}^{c}_{(a,b)} \ \phi & := & c \ \mathsf{k} \ M \wedge M \ \mathsf{proofFor} \ \phi \\ (M, (M', I)) \ \mathsf{iProofFor}^{c}_{(a,b)} \ \phi & := & M' \supseteq_{(a,b)} M \wedge (M', I) \ \mathsf{iProofFor}^{c}_{(b,a)} \ \phi \end{array}$$

Possible Application to Zero-Knowledge Proofs (1/3)

2-party *Interactive* Provability

$$\mathsf{IP}_{(a,b)}(\phi) := \exists m(m\ \mathsf{iProofFor}_{(a,b)}\ \phi)$$

Zero-Knowledge proofs (definition)

"Zero-knowledge proofs are defined as those [interactive] proofs that convey no additional knowledge other than the correctness of the proposition [ϕ] in question." [GMR89]

$$\begin{aligned}\mathsf{ZK}_{(a,b)}(\phi) := \mathsf{IP}_{(a,b)}(&\mathsf{K}_a(\exists m'(\mathsf{K}_b(m'\ \mathsf{proofFor}\ \phi))) \wedge \\ &\neg\exists m''(\mathsf{K}_a(\mathsf{K}_b(m''\ \mathsf{evidenceFor}\ \phi))))\end{aligned}$$

Possible Application to Zero-Knowledge Proofs (2/3)

Zero-Knowledge proofs (properties)

Spelled out, a (the verifier) knows through interaction with b (the prover) that b knows a proof (m') for the proposition ϕ, however a does not know that proof nor any evidence (m'') that could corroborate the truth of ϕ. (Observe the importance of the scope of the existential quantifiers.) Philosophically speaking, a has *pure propositional* knowledge of ϕ, i.e., a has *zero individual* (and thus *zero intuitionistic*—no witness!) knowledge *relevant* to the truth of ϕ. In Goldreich's words, it is "as if [the verifier] was told by a trusted party that the assertion holds" [Gol05, Page 39].

Possible Application to Zero-Knowledge Proofs (3/3)

Zero-Knowledge proofs (conjecture)

"[A]nything that is feasibly computable from a zero-knowledge proof is also feasibly computable from the (valid) assertion itself." [Gol05, Page 39]

$$\models \phi \to ((\mathsf{K}_a(\varphi) \supseteq \mathsf{ZK}_{(a,b)}(\phi)) \to (\mathsf{K}_a(\varphi) \supseteq \phi))$$

*I*nteractive evidence & Belief

2-party *interactive* evidence

$$
\begin{array}{rcl}
M \ \mathsf{iEvidenceFor}_{(a,b)}\ \phi & := & M \ \mathsf{iEvidenceFor}^{a}_{(a,b)}\ \phi \\
(M, \blacksquare)\ \mathsf{iEvidenceFor}^{c}_{(a,b)}\ \phi & := & c \ \mathsf{k}\ M \wedge M \ \mathsf{evidenceFor}\ \phi \\
(M, (M', I))\ \mathsf{iEvidenceFor}^{c}_{(a,b)}\ \phi & := & M' \supseteq_{(a,b)} M \wedge (M', I)\ \mathsf{iEvidenceFor}^{c}_{(b,a)}\ \phi
\end{array}
$$

2-party *interactive* Belief

$$
\mathsf{IB}_{(a,b)}(\phi) := \exists m(m \ \mathsf{iEvidenceFor}_{(a,b)}\ \phi)
$$

Conclusion

1. Modern cryptography is cryptic due to its machine-based definitions.
2. This deep-rooted problem must be administered a radical remedy: **redefinition**.
3. Modal logic is a good candidate remedy.